LA-UR-21-29730

Title: Fiber Optic Seal Based on Spectral Interferometry for IAEA

Author(s): Pickrell, Mark Manley
Gilbertson, Steve Michael
Kalb, Daniel M.
Koppi, Anthony Charles

Intended for: Report

Issued: 2021-09-30

Los Alamos
NATIONAL LABORATORY

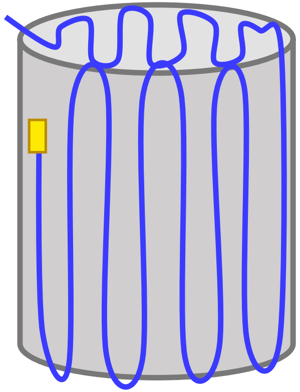
Fiber Optic Seal Based on Spectral Interferometry for IAEA

Steve Gilbertson, Dan Kalb, Anthony Koppi, Mark Pickrell, J-4

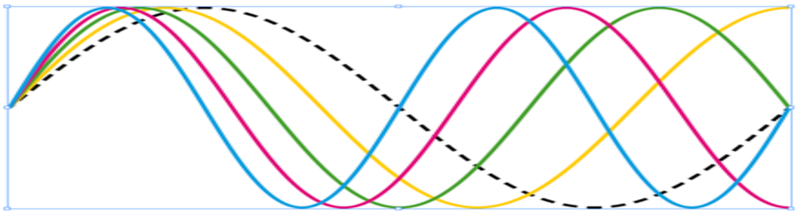
October 1, 2021

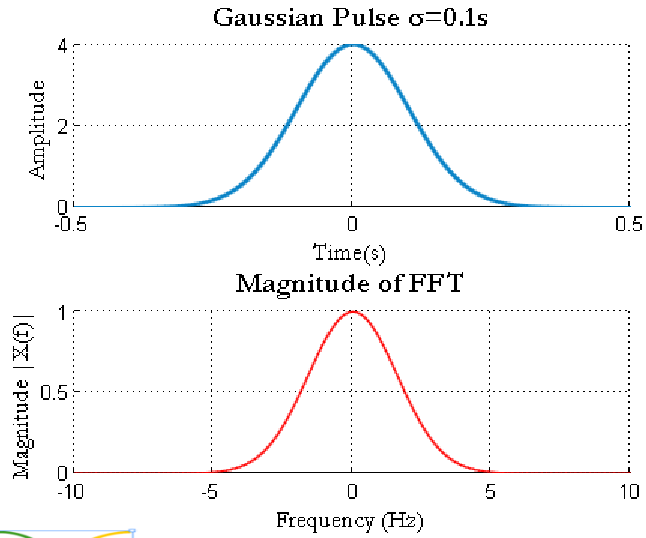
Introduction: Technology Evaluation and Demonstration: A Robust Tamper-Indicating Seal

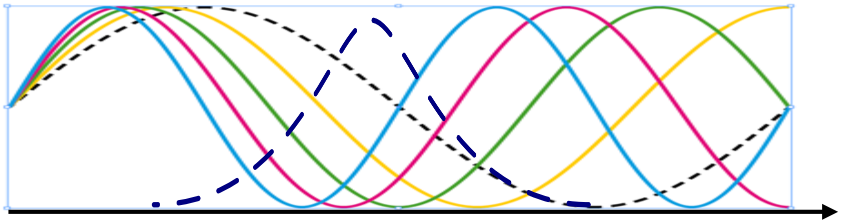
- Objective was to develop a robust, tamper-indicating seal for IAEA (or similar applications).
- Fiber-optic based.
- Existing optical fiber seals do not have an encoding of the light signals that could render them tamper-proof.
- This seal is based on wave-mechanics to encode the light signals.
- Defense in depth design.
- Passive or active design. Passive demonstrated here.
- Prototype system complete. Requires final configuration and technology transfer.



Physics Background: Wave Mechanics

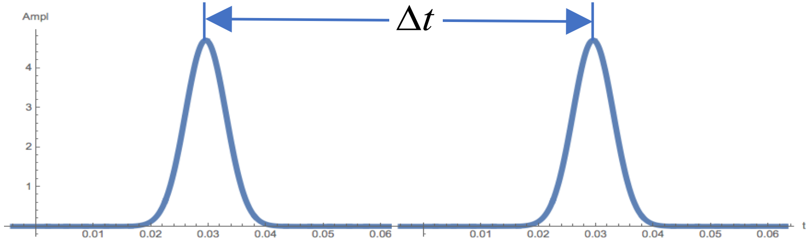


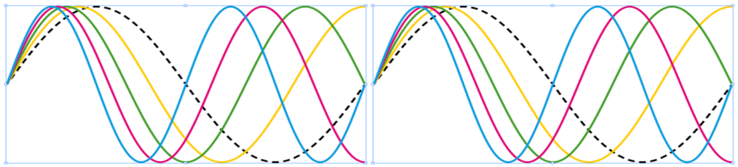


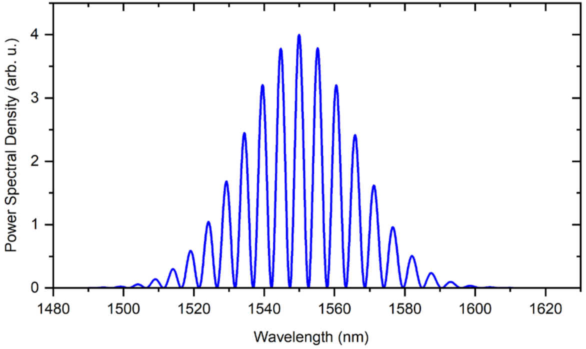


The Fourier Transform of a short laser pulse is a spectrum of waves (near the laser wavelength), extending infinitely in time (mathematically).

Spectral Interference: Now Consider 2 Laser Pulses

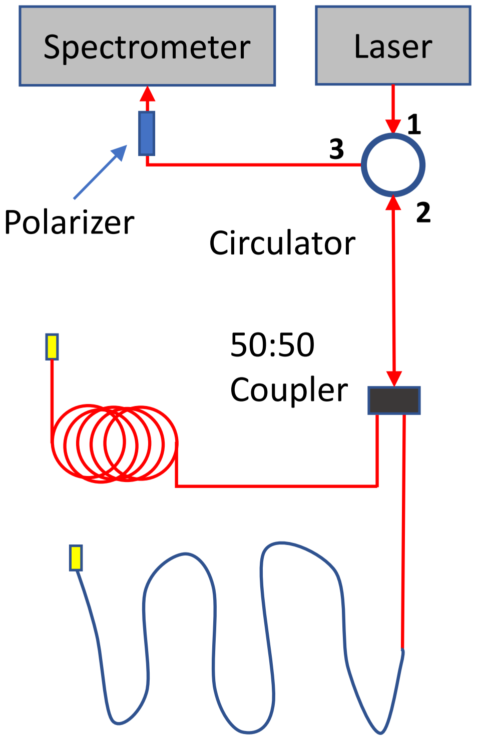




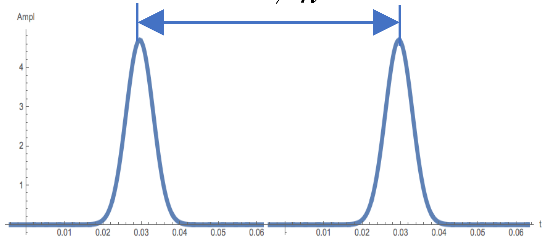


- Close, but not overlapping in time.
- But, Fourier Spectra are overlapping (long duration, infinite mathematically).
- Fourier wavelengths interfere.
- Phase difference because of time separation.
- Destructive and constructive.
- Interference in <u>wavelength domain, not time domain</u>.
- Measure with a spectrometer
- Optical encoding.

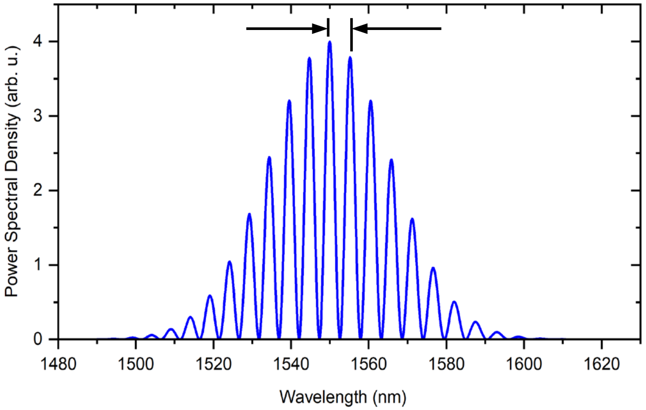
Now Consider a Basic Interferometer (Michelson)



$$\Delta t = \frac{\Delta x}{c/n}$$

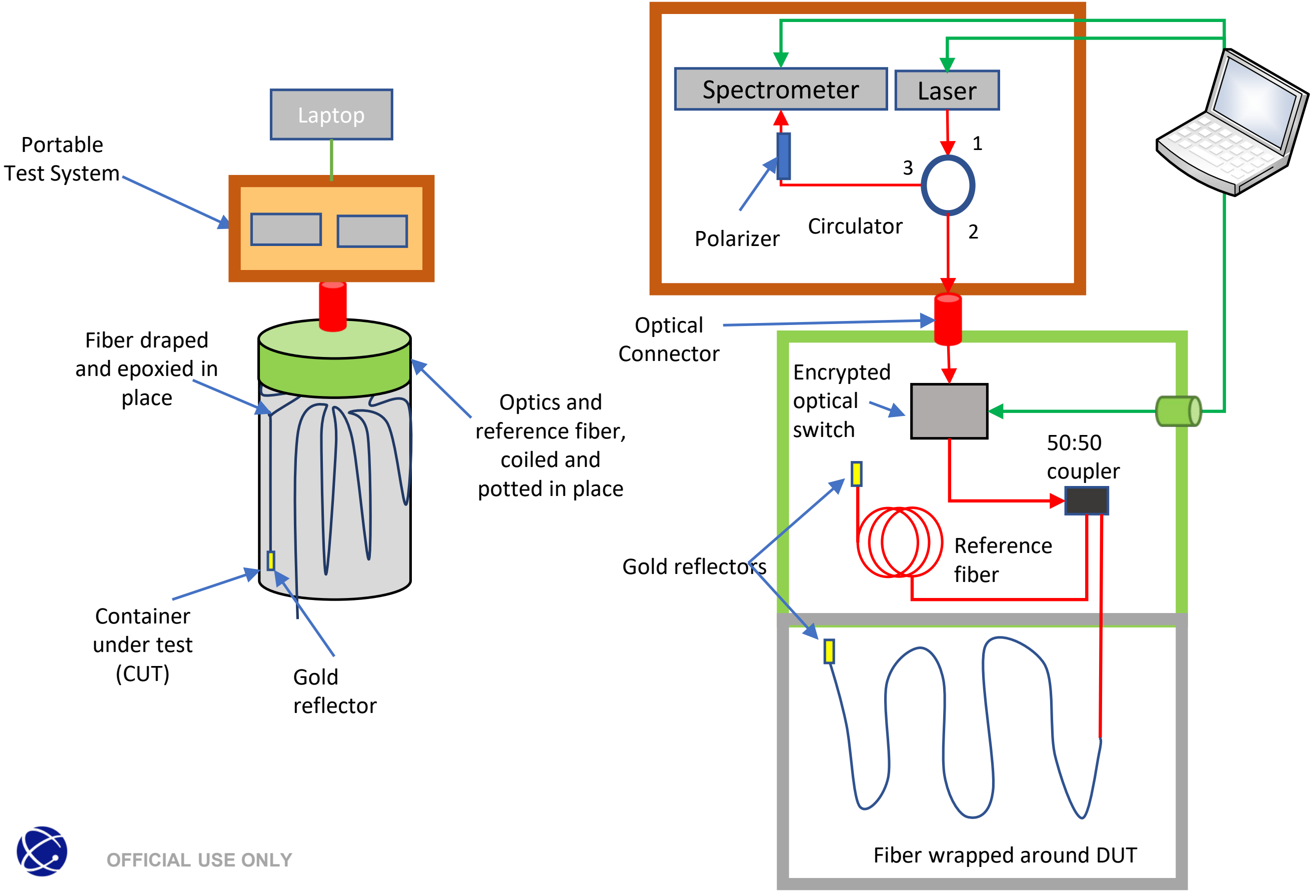


$$\Delta\lambda = c\Delta t$$



- Pulse is split into 2, then sent through fibers, reflect, and recombine.
- Different path lengths separate pulses in time.
- Fourier components interfere.

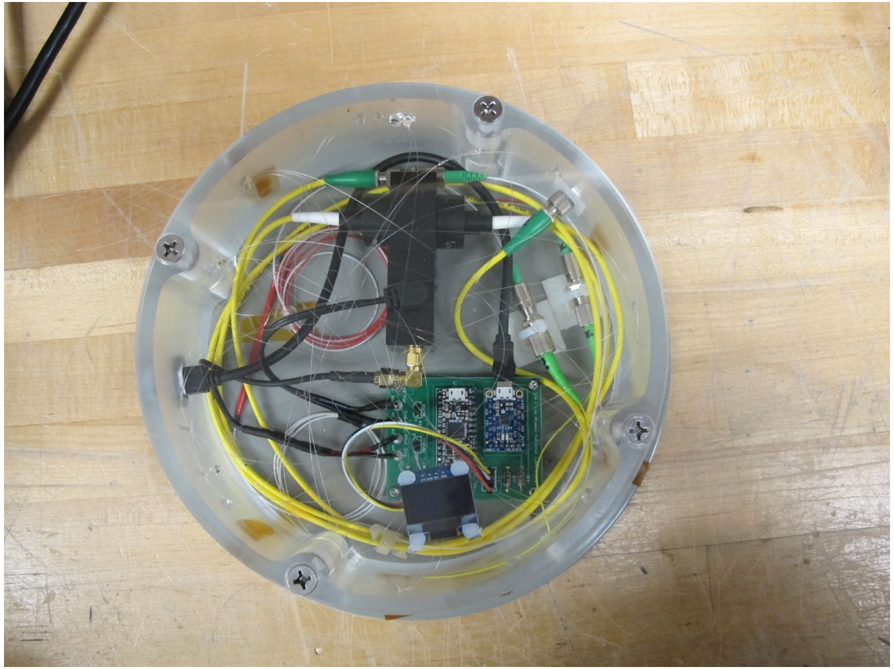
The Fiber Optic Seal is Based on the Same Principle



- Optical topology is identical except:
  - Encrypted optical switch.
- Reference fiber is used to protect the seal enclosure
- Reference and DUT fibers are equivalently tamper sensitive.
- Spectrometer and laser are removable.

The Seal. Permanently Attached

- Total production cost: $200 - $900
- Attach to item being protected.
- Fiber should be epoxied to item, or embedded in a protective sheet, or some other method.
- Passive seal, but can be active.
- Reference fiber leg is part of seal and is used to protect seal body. Helps to eliminate temperature fluctuations.

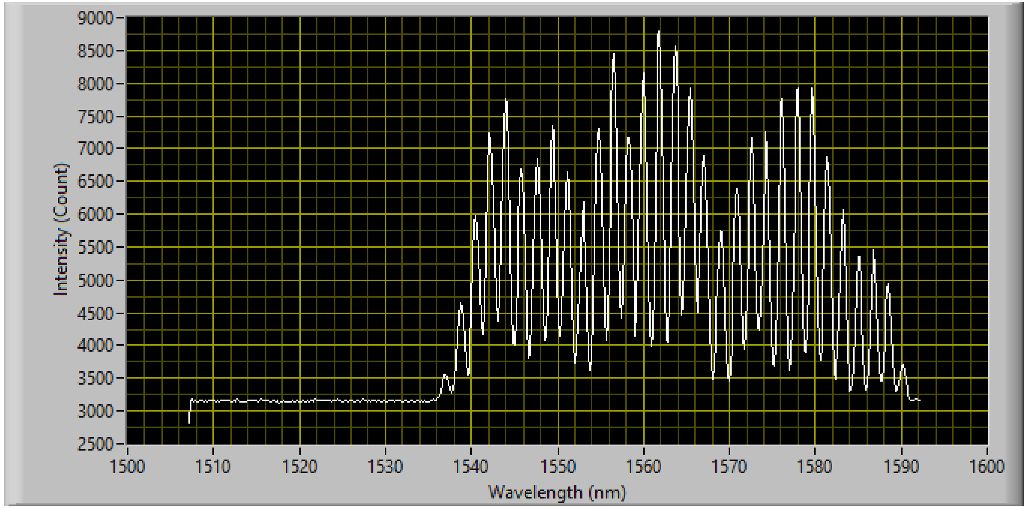


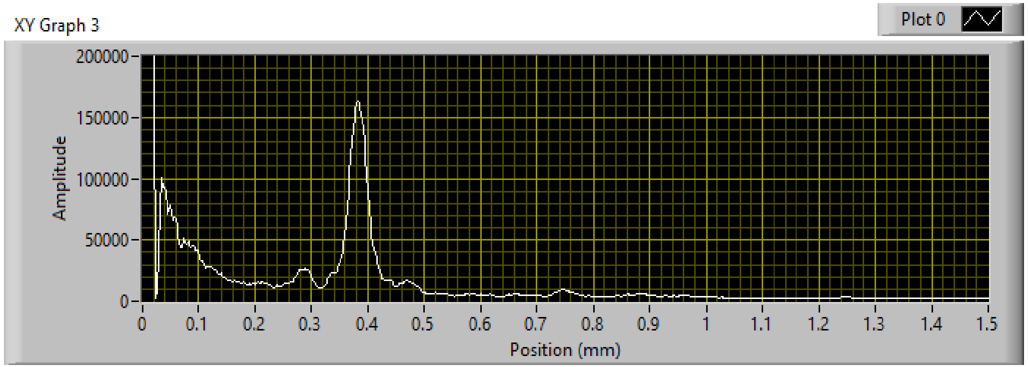
Interrogation System

- Carried by inspector.
- Lightweight: just this plus laptop
- Must include access key for optical switch.
- Attaches to seal by fiber optic cable.
- Attaches to laptop by USB cables.
- Laser pulse frequency: 100 MHz
- Spectrometer averages over multiple pulses.
- Software acquires data and performs FFT for length

Data From Our System

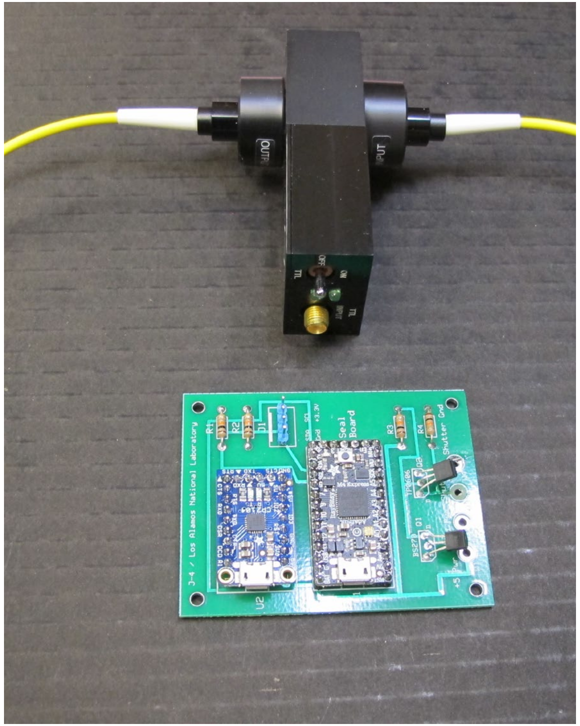
- Data taken on Laptop with our custom software.
- Top trace is interference spectrogram. Intensity vs. Wavelength
- Bottom trace is FFT of spectrogram. Shows Δx
- Resolution is 20 microns.
  - Human hair is 80 microns.
- Detection level can be set larger if 20 microns is too small.





What is the Optical Switch For??

- For the <u>passive</u> system, we considered that an adversary could attach an LUNA™ swept wavelength interferometer to the optical connector between inspections and measure the optical lengths of the reference and test fibers. Then the adversary could, in principle, duplicate the fibers (accurate to 20 microns) and replace the seal in its entirety.
- We installed an optical switch which blocks the optical path except for authorized measurements.
- The optical switch is controlled by a microcontroller. The laptop connects to the microcontroller through an interface and sends it a key code. Only when the proper key code is received will the switch allow the optical signal to pass.



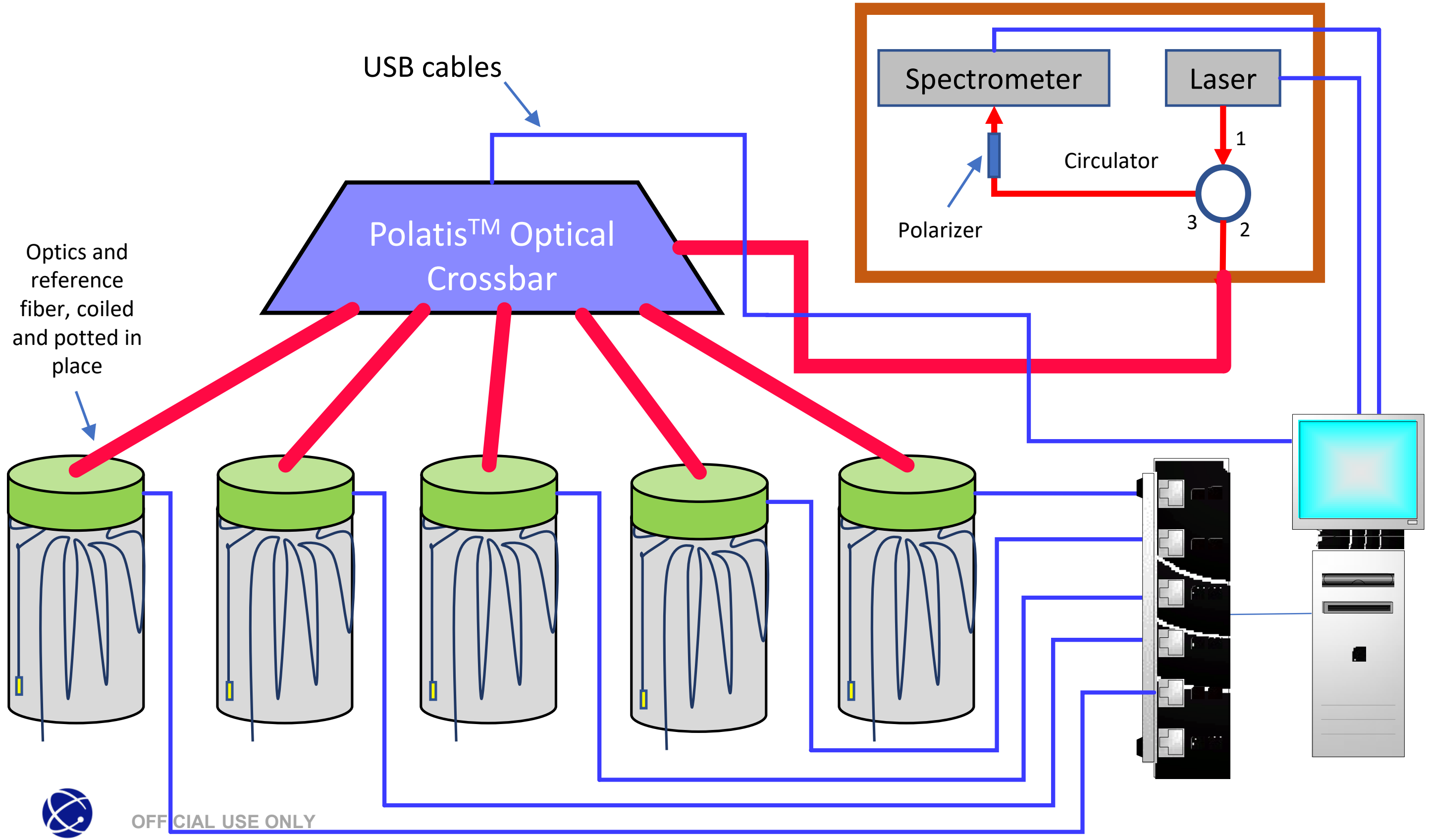
Operating Process

- Attach a new seal to the device to be protected.
  - The fiber should be epoxied in place, or part of an enclosing sheet.
    - The fiber is somewhat delicate and must be integrated properly.
- Connect the interrogation system with an optical fiber.
- Connect the Laptop with USB cables to the seal and interrogation system.
- Program an access key phrase into the analysis software and seal.
- Measure the seal for several seconds.
- Record the seal measurement and key phrase in the software.
- Subsequently, to inspect the seal for tampering:
  - Attach the interrogation unit and Laptop as before.
  - Provide key phrase to enable the optical switch.
  - Make the measurement.
  - Compare to baseline.

Tamper Sensitivity of the Fiber

- This analysis assumes the passive application: separate measurements.
- If the fiber is cut, the interference pattern is lost.
- If the fiber is stretched by more than 20 microns, the interference pattern is significantly changed.
- The precision is excellent. The spectrometer integrates over thousands of pulses. Laser pulse rate is 100 MHz.
- If the fiber is cut then re-welded, some of the fiber glass is lost and the fiber is shortened, typically by a couple of millimeters. The interference patter is entirely different.
- If the fiber is damaged, then a new local reflection point is created that modifies the interference pattern.
- Temperature changes do not affect the interference strongly because <u>both</u> fibers will change.

Another Configuration Could Be The Semi-Active



- Use a Polatis™ Optical Crossbar switch.
  - Coherence preserving
  - Minimal insertion loss
  - Sequentially selects each seal.
  - ~1 sec. each

Our (Very) Preliminary Vulnerability Analysis Assume Passive Case

- The adversary could attempt to cut the fiber to access the container.
  - The system would detect the cut because the signal would be lost.
- The adversary could attempt to cut and then re-weld the fiber.
  - It is easy to re-weld the glass fiber, but a significant amount of fiber material is lost in the process, nominally a few millimeters. The system is sensitive down to 20 microns, or a 100 times more resolved than the loss.
- The adversary could attempt to move the fiber to the side, perhaps cutting the enclosing sheet.
  - Even slightly stretching the fiber (it is mostly plastic deformation) will be detected if it is greater than 20 microns.
- The adversary could attempt to measure the optical lengths of the two fibers using a LUNA-type device.
  - The encrypted optical switch would prevent this.

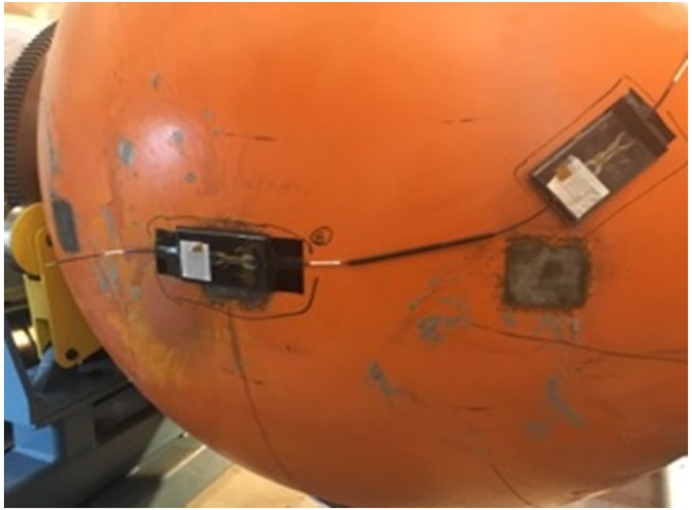
Our (Very) Preliminary Vulnerability Analysis (Continued). Assume Passive Case

- The adversary could attempt to reproduce the entire seal.
  - This would fail for several reasons. Without knowing the lengths of the two fiber legs to within 20 microns, the adversary could not reproduce the interference pattern. Moreover, the adversary could not match the key for the encrypted optical switch.
- The adversary could attempt to penetrate the seal body to activate the optical switch and then measure the fiber lengths.
  - The penetration would destroy or damage the reference fiber, which is wound on the inside of the seal container. Then, the LUNA measurement would be impossible.
- The adversary could attempt multiple passwords to enable the optical switch and obtain optical access to the fibers.
  - The number of potential passwords is enormous if a long password is used. We can put in a software delay of 1 second between attempts.

$$N_p = \sum_{n=1}^{m} 128^n = \frac{128^{m+1}}{127}$$

But… The Fiber is Very Delicate

- Yes, by design.
- Sensitivity proportional to “delicateness.”
- This system has to be integrated into the over all seal.
- For example, we epoxy fibers to explosive blast containment vessels ⇒
  - Used at DARHT to contain hydrotests with 45 lbs. of HE.
- Could also be built into a shroud or heavy plastic bag.
- Another aspect of prototype, such as clear covers of seal and interrogation unit.



Application Summary

- Exceptionally resilient to undetected tamper.
  - Wave mechanics encoding of optical signal.
  - Overall design.
- Laser / optical components are all COTS, standard telecommunications technology.
- Nominal production costs:
  - $200 - $900 for seal
  - $50k for interrogation system
- Passive seal in this configuration
  - Can be used actively
  - Can be used semi-active with optical cross-bar switch.
- Next step would be customer specification of specific configuration.